Title

Anti-Alternation System for Homepage

Background of the Present Invention

Field of Invention

The present invention relates to web server computer system on Internet, and more particularly to an anti-alteration system for homepage adapted to prohibit the homepage from illegally change.

Description of Related Arts

Internet based TCP/IP protocol, can provide communication environment to computer user anywhere on network easily. This advantage also is a disadvantage with security.

Web server can save all multimedia files which include image and sound files (html, text, gif, jpeg, au etc.) and at user browser side computer executable file in hard disk. It will return it when get a request from user's browser, which also easily allows to be illegally changed if hark be invasion the web server computer by any way.

To avoid this attack, there is a way that only authorized user can access web server files and this also can avoid virus attack.

However, we must allow all users to access the web server on Internet and such way will setup a lot of limitation on it. Internet is built by an architecture by using telnet or ft session to reply the request and it is difficult to check authorization for all access. It is because HTTP protocol is different from other transmission applications, such as TELNT, FTP.

As one of the anti-illegally attack technologies, it is necessary to create a homepage monitor system. The basic idea is periodically checking all web files

(homepage) from the web server which are illustrated as following orders, as shown in Fig. 1:

P1->P2->P3->.....Pi->.....->Ps->.....->Pn->P1->P2->...

If there is illegally changed, it may be recover the illegally changed files or stop the web server.

As a problem of the above technology, it still could send some illegally changed web file to user because it takes many time to check all files. In this time, if an access request is received from the user, then the illegally changed file will be send to the user.

When increasing pages of data, it takes over 10 minutes to check all web files. During such 10 minutes checking, illegally changed data has been sent to user. In other words, the illegally changed of web files can't be avoid in 100%.

Moreover, the former technology must always keep monitor server running under heavy utilization which will delay the response. It is also not suitable for large server with many files.

Summary of the Present Invention

A main object of the present invention is to provide an anti-alteration system for homepage which can prevent web server sending illegally changed data to user absolutely.

It is another object of the present invention to provide an anti-alteration system for homepage, which can prevent Harker from invading a web server and any illegally changing of web file on any meaning.

It is another object of the present invention to provide an anti-alteration system for homepage, in which it does not need to stop functioning when it has to maintain homepage files at web sit.

It is another object of the present invention to provide an anti-alteration system for homepage, which is built at the application layer so that it is easy to transplant between different OS platforms (for examples: WindowNT, Window2000, Window98, SOLARIS, LINUX, etc.).

It is another object of the present invention to provide an anti-alteration system for homepage, which is easy to installation and does not need modify the existing web server and homepages.

It is another object of the present invention to provide an anti-alteration system for great web homepages, wherein the encryption is the encryption using chaos theory (for example: using GCC chaos encryption) and the massage authentication technology is using chaos theory (for example: using ChaosMAM).

In order to accomplish the above objects, the present invention provides an anti-alteration system for homepage, which comprises:

a public-web-server computer which retention the safe-web-files encrypted from the usual web files (html, txt, gif, jpg, jpeg, au, exe, etc.);

an original-web-server computer which retention the usual web files that connecting the public-web-server computer though a means for preventing illegally access as well as firewall;

means for checking and decrypting and sending which while receiving the user's requested, wherein a web server in the public-web-server computer checks a safe-web-file, wherein if the result be un-illegally altered, then the web server sends back the web-file deciphered from the safe-web-file to the user; and

a recoverable means for encrypting the web file to the safe-web-file on the original-web-server computer, and automatically recovering changed the safe-web-file in the public-web-server, when the safe-web-file is illegally altered and checked out by the public-web-server.

Alternatively, a second embodiment of the present invention provides an anti-alteration system for homepage, which includes:

a public-web-server computer having a prohibit homepage illegally alter function, which retains the safe-web-files that have been added with the prohibit illegally alter header's information, including a MAC (Massage Authentication Cord) generated authentication checking whole web-file and properties including name, size, date, location, etc. thereof;

an original-web-server computer retaining the web-file connects to the public-web-server computer which is added with the prohibit illegally alter and decrypt functions, though a means of avoiding illegally access as well as firewall;

a real-time-check technique, in which when a user's requested is received, the web-server in the public-web-server computer separates the header information from the requested safe-web-file which is added with avoiding illegally alter header, and at same time using the MAC(Message Authentication Cord) which is included in the header information to check the safe-web-file by means of a message authentication technology;

as this means, wherein when the user's requestion is received, the real-time-check technique is used to check the safe-web-file and, if the result is un-illegally altered, the header information is cut from the safe-web-file and then changed to a usual web-file which is sent back from the mirror-web-sever computer to the user's browser based http protocol; and

a recoverable means for adding the header information to the correspondence web-file to make a new safe-web-file on the original-web-server computer when the illegally altering of the safe-web-file is detected, wherein such new safe-web-file is sent to the public-web-server computer to automatically recover changed safe-web-file.

Alternatively, a third embodiment of the present invention provides an anti-alteration system for homepage, which includes:

a public-web-server computer having a prohibit homepage illegally alter function, which retains the safe-web-file that are encrypted from the web-file and has been added with the prohibit illegally alter header's information including the MAC (Massage Authentication Cord) generated authentication checking the whole web-file and the properties(name, size, date, location at harddisk, etc.) of the web file;

an original-web-server computer retaining the web-file and connecting the public-web-server computer which is added with prohibit illegally alter and decrypt functions, though a means of avoiding illegally access as well as firewall;

a real-time-check technique, in which when a user's requestion is received, the web server in the public-web-server computer separates the header information from the requested safe-web-file which is added with avoiding illegally alter header, and at same time, the MAC(Message Authentication Cord) included in the header information is used to check the safe-web-file by means of a message authentication technology, wherein when the user's requestion is received, the real-time-check technique is used to check the safe-web-file and, if the result us un-illegally altered, the head information is cut from the safe-web-file and then decrypted to a usual web-file which is sent back from the safe-web-file to a browser based http protocol of the user; and

a recoverable means for encrypting and adding the header information to the correspondence web-file when the illegally altering of foregoing safe-web-file is detected, so as to make a new safe-web-file on the original-web-server computer, which is sent to the public-web-server computer to automatically recover changed safe-web-file.

Alternatively, a fourth embodiment of the present invention provides an anti-alteration system for homepage, which includes:

a public-web-server computer retaining the safe-web-files that have been encrypted and added with the prohibit illegally alter header's information, including a MAC (Massage Authentication Cord) generated authentication checking whole web-file and properties including name, size, date, location at harddisk, etc. thereof;

a CGI Gateway module for sending the request information to a CGI Gateway means, in which when the public-web-server computer gets a request information from user's browser to executes a CGI (Common Gateway Interface) program, the request information is URL format including IP address, comment and parameters etc, however said public-web-server does not execute the CGI program before doing generation process, send the request information to the CGI Gateway module only; and

a send request information to original-web-server means, in which at the CGI Gateway module, the request information is modified to a new request that is able to be

received by an original-web-server automatically and such new request is sent to the original-web-server computer;

means for using the modified request information got from the CGI Gateway module and the original-web-server executing the CGI program in the original-web-server computer; and

means for outputting a http header and CGI contents from the CGI program which are sent from the original-web-server to the CGI Gateway at the public-web-server computer; and

means for sending back the CGI output from the CGI Gateway module to the user's browser passing through the public-web-server or directly.

A fifth embodiment of the present invention is an alternative mode of the above first to fourth embodiments, wherein a chaos encryption technology(as GCC chaos encrypting) is applied to the encryption/decryption because it is most fast and most safe then another encryption.

A sixth embodiment of the present invention is an alternative mode of the above first to fourth embodiments, wherein the real-tim-chech technique uses a message authentication technology employing chaos theory.

Brief Description of the Drawings

Fig. 1 is a schematic diagram illustrating an alter check method according to a conventional technology.

Fig. 2 is a block diagram illustrating an anti-alteration system of the present invention.

Fig. 3 is a block diagram illustrating a message authentication of the present invention.

Fig. 4 is a schematic diagram illustrating a structure of a safe-file of the present invention.

Fig. 5 is a block diagram illustrating a structure of a usual web server.

Fig. 6 is a block diagram illustrating a structure of a web server in public-web-server computer employed with a real-time-check module of the present invention.

Fig. 7 is a block diagram illustrating principles of real-time-check module/module of the present invention.

Fig. 8 is a block diagram illustrating usual execution principles of CGI program.

Fig. 9 is a block diagram illustrating principles of alter prevention of CGI programs of the present invention.

Fig. 10 is a block diagram illustrating a system configuration of the homepage anti-alteration system using GCC (Gao's Chaos Cryptosystem) Chaos Encryption and Chaos MAM (Message Authentication Method) technic in implementation embodied in the present invention.

Detailed Description of the Preferred Embodiment

Fig. 2 illustrates an overall concept of the system of the present invention. The present invention performs authentication check over the whole web file. If the authentication check detects any alteration, it stops sending the illegally changed web file. It enables system administrators to deal with the alteration immediately while the system is equipped with means to inform administrators of the alteration.

The present invention that encrypting web server would not distribute any illegally altered data to Internet user (browser in software terms). In the present invention, the web file is maintained as encrypted and added with the prohibit illegally alter header's information while being sent to users. It is decrypted once it receives page access request. Using this method, even if the system attacker alters the page data, it cannot send the altered content to users directly. This is because the content became meaningless once being decrypted as the page data sent to users is decrypted. As far as the attacker does not alter page data in its encrypted form, he or she cannot let this web server send any altered yet meaningful content to any users.

The web file stored in the public-web-server that is equipped with the alteration prevention function is open to the Internet users. The web-file stored in the original-web-server is kept for maintenance, administration, and/or file-backup purposes. In other words, to add or modify a homepage, the administrator first implements the change to the web file stored in the original-web-server. After that, the change will be encrypted and transferred to the web file in the public-web-server that is equipped with the alteration prevention function. The original web file in the original-web-server cannot be opened nor accessed directly by the Internet users.

Once alteration is detected, the web file containing the altered data can be automatically replaced with the original web file since the system has one private original-web-server and one public-web-server equipped with the alteration prevention function. In other words, the homepage can be automatically reinstated.

Authentication is a technology ensuring the completeness and correctness of information. While encryption ensures the secrecy of the information, authentication aims

at ensuring that the information has not be changed. Authentication includes message authentication, user authentication, terminal authentication, and time authentication and so on. Chaos MAM is a new Message Authentication Method (MAM) using Gao's Chaos Cryptosystem (GCC).

In other words, in dealing with the plain text M in the original-web-server, the authentication technology employed in ChaosMAM creates a MAC (Message Authentication Code) based on the plain text M and then compares it with the MAC' created in the web server that is equipped with the alteration prevention function. If MAC' is found to be different from MAC, the system determines that an alteration has occurred and the web server equipped with the alteration prevent function will request M from original-web-server and replace the altered M' with M.

Performing message authentication can prevent this from happening. As shown in Fig. 3, in message authentication, sender creates MAC (Message Authentication Code) from outgoing message using a crypt key and then sends both the message and MAC. The receiver receives message M', which may not be identical to M due to potential alternation en rout, creates MAC' from the message M' using a same crypt key (may be need to use public key technology to send the crypt key from sender to receiver), and compares MAC with MAC'. If they are the same, the message is authentic. Otherwise the message was altered.

Fig. 4 shows the construction of the safe-web-file of the present invention. Header information like MAC, size, dates, properties, address of the file is stored in the web file. The system of this invention can also be built, in principle, with various other encryption systems and message authentication technologies, though the system based on GCC and the authentication technologies using GCC is the most superior from the processing speed perspective.

The actual examples using MAC is explained. Then, the example of correcting altered web file and sending it to users real-time is explained.

The principle of the web server with the function of real time check revealed in the present invention is explained. It is well known that the primary function of the web server is to send web files of requested homepages to clients, or said browsers. In most cases, the requested web file is stored in a hard disk and can be easily accessed from a

server. The web server seeks out the file based on the request and transfers its content to the HTTP address of the client system that made the request.

Fig. 5 shows the principle of a regular web server which includes:

1). An initiation process such as inputting environmental parameters.

2). Receiving request that be URL format from web browsers using http protocol.

3). Reading requested file from hard disk after necessary processing work.

4). Sending to web browser the contents of the requested file.

The web server of the present invention, as shown in Fig. 6, is the engine of the homepage anti-alteration system. It inserts the real_time_check module between the Openfile module and the send module. The Openfile module reads the web file referred to above from a hard disk and writes it into the computer memory.

Fig. 7 shows the principle of the real_time_check module. Based upon the request information, the module first inputs a file attached in the alteration prevention header into the memory. The header consists of a MAC (Massage Authentication Cord) generated authentication checking whole web-file and properties including name, size, date, location at harddisk, etc. thereof.

Whether a file is altered or not is checked by the Message Authentication Technology. If the file is not altered, the portion containing alteration prevention header is dropped, the file is decrypted and then sent to browser.

If the file is altered, the system requests recovery from the recovery server in the original-web-server. The recovery server encrypts the original web file stored in the directory of the original-web-server selected by the request information. Then it creates MAC using the Message Authentication Technology, and puts the information of the file, like its size, date, time, and properties into the alteration prevention header. This file is sent to the public-web-server. Because of this, the altered file stored in the public-web-server can be recovery and updated. The updated or corrected file is sent to the browser.

Because they will be detected by message authentication check before being sent, altered files will never be sent to web clients at all.

The system of this invention for the first time achieved the "real_time_check" technology. In other words, the alteration prevention web server revealed in this invention places little additional burden on CPU of a computer because it conducts checks on the requested file only and before sending it out.

However, to realize the practical real time check technology, high-speed/high strength encryption and authentication check technology is necessary. The present invention achieves the highest level of homepage alteration prevention system by incorporating GCC (Gao's Chaos Cryptosystem) cipher and ChaosMAM technologies known for their high processing speed.

In view of above, the real_time_check technology is a very effective technology in handling execution files at browser sides and various web files containing pictures, sounds, extensions like HTML, html, Text, GIF, JPEG, au, etc.

However, in dealing with CGI files, other methods have to be considered. CGI (Common Gateway Interface) is a program executable through web server. It is called CGI script or CGI file also. CGI is a gateway interface independent of language and can be implemented using any application development language like C, C++, Perl, and even JAVA. Its extensions are defined like .pi, .cgi, or .exe.

The CGI program was developed for web server administrators and its expert users to add special features/functions. The usage varies. For example, it can take DATA from a database server in another computer, compile it (or summarize, statistically analyze, graphic construct, etc.), and then send the results out. It can handle more complicated tasks. CGI program can execute executable files like OpenText, and send the results to browsers.

The execution of the CGI program includes the following:- corresponding to the request in forms of URL from a client; executing the program in the web server environment; and sending the results to the browser used by the client.

As shown in Fig. 8, the flow includes the following steps.

1). Set environment parameters for the CGI program. Set the parameter name of request method of HTTP as REQUEST_METHOD, and set the data taking from client as QUERY_STRING.

2). Execute the requested CGI program using request information got from user.

3). Wait for the completion of CGI program, read the output from STDOUT, and analyze it, and stop the Content-Type.

4). Create the necessary HTTP header.

5). Send the header and the output of the CGI program to the client who made the request.

The homepage anti-alteration system proposed in the present invention is constructed from a public-web-server and an original-web-server. The original-web-server stores non-executable files like HTML, TEXT, GIF, JPEG, and CGI files. Though the original-web-server can be run as a usual web site, the system of the present invention uses it as the storage location for original files only.

The non-executable files putted on public-web-server computer are enciphered and added MAC. We can prevent to alter web site by using real time check technology on web server. But it is different for CGI programs. Because execution of CGI programs are depend on the execute environments of original-web-server computer, such as OS, IP address, directory structures and so on. When they are moved to public-web-server from original-web-server, the execution environments (such as IP address, directory etc.) will be changed and many times they cannot be executed. So, in the present invention, a new proposal is shown to solve the problem of CGI programs as follows.

We use usual web server (for example: Apache, Netscape, etc) for original web site, and original web files such as usual html file, GIF and CGI files reside in it. In public-web-server computer, there is a web server modified not to directly execute CGI program. And we add CGI Gateway module. We will not put CGI files in public-web-server computer.

Referring to Fig.9, the process flow of CGI in the present invention is illustrated

as follows.

(1) In the public-web-server computer, environment variables for CGI programs are set up. The request method name of HTTP to REQUEST_METHOD environment variable and the set data received from client to QUERY_STRING environment variable are set up.

(2) Pass the request information of CGI program (IP address, comments, parameters, etc.) received from browser to CGI Gateway module.

(3) In CGI Gateway module, modify automatically received request information to be acceptable by original web site, then send the new request to execute CGI file to original-web-server.

(4) In original-web-server, execute the requested CGI program on original computer as usual.

(5) Send http header and output of CGI program to CGI Gateway module on public-web-server.

(6) CGI Gateway module send output of CGI program to browser through public-web-server or directly.

An example of implementation of the present invention with using GCC Chaotic Encryption System and ChaosMAM chaotic authentication technology is disclosed as follows.

First, the Chaotic Encryption System is briefly explained. One can use either of Public-key encryption system or Symmetric-key encryption system in Chaotic Encryption System. Symmetric-key encryption system will be used for explanation here. In the present invention, it is no need to give key to the user, so it will be enough by Symmetric-key encryption system. Assume plain text P, chaotic cipher function G, ciphered text C, cipher key K. It can encipher as

$$C=G(K, P)$$

To decipher the ciphered text C, with using reverse function G^{-1} and key K we can decipher as

$P=G^{-1}(K, C)$

In chaotic encryption system, one can use arbitrary length of plain text P. The length of key K is variable and from 8 bit to 2048 bit, and have not any effect to speed.

The present invention consists of some parts including

(1) Public-web-server,

(2) Encoder/Decoder module,

(3) Recovery server and Recovery client,

(4) Alert system,

(5) Policy management system and etc..

At there

(1) Public-web-server includes decoder functions additional to all usual web server (for example Apache).

(2) In Encoder/Decoder module, encoder part does encipher, addition of MAC, addition of header information, etc. and decoder part does authentication check, decipher, strip off header information, etc.

(3) Recovery server includes encoder functions.

In Fig.10, a conceptual system configuration of homepage anti-alteration system by encipher of web files of the present invention is illustrated. Basically it is similar configuration as shown in Fig. 2. But it is different in that web files in public-web-server computer with alter prevention function are enciphered, updates of safe-web-files are done through Recovery client, and Chaotic Encryption System is used for encipher, and

ChaosMAM is used for generating MAC and doing authentication check.

Web files including Homepage's HTML files are held in original-web-server computer. Do Encoder for them through Recovery server. It consists of GCC encipher of web files, generation of MAM MAC(MAM MAC: it means MAC by Message Authentication Method) and addition of header information part including file size, date, MAC, etc. Send them to Recovery client installed outside firewall and controlled under Recovery server.

Recovery client put the received encoded web files to the place indicated by Recovery server. When issued request for homepage from network users, web server with alter prevention function will

(1) Read out MAC etc. information from header part of encoded web files, and

(2) Do decoder operation such that it does authentication check for the web files.

If that passed authentication check, it strips off header part from the files and enciphers them. Then it sends recovered web files to the users.

If it has seen alteration at authentication check, it will do recovery actions such that it issues the request to update the altered file to the Recovery server through the Recovery client. The Recovery server get specified file from usual sever in respond to the request, encode it, and send to server with alter prevention function. At the same time, it informs the facts to the Alert system, and the Alert system informs the existents of invader for system administrator through public line.

There are following merits in the present invention.

(1) There is no CGI file in public-web-server computer. So, even if Hacker invades to this public-web-server, he/she cannot alter the CGI file or executing his/her CGI file.

By the way, Hacker cannot invade to original-web-server computer, because the original-web-server computer does not open to the public users (conceived), it is used usual firewall between public-web-server computer and original-web-server computer. So,

it is considered that CGI file in original-web-server computer is safe.

(2) CGI programs can execute in original-web-server computer with current environments. For developers of web site, installation, daily update and maintenance of homepage alter prevention system of this invention is very easy because they can use current operations to update home pages.

(3) You can use current way to issue the requite for execution of CGI program to public web site as public user who access home page of the web site.

(4) It can deal well various CGI made by C, C++, Perl, Java, etc. computer languages. Especially, it can deal Fast CGI by its principles.

With the system of this invention, you can get following results. The present invention realizes the technology of web real time check. As a speed, this will do authentication check and decipher instantaneously, at the moment it received the request from browser, so response time is almost same as the case without the check system. As a safety, it will not send altered file to outside (browser side) absolutely, if there is alteration action.

For large systems, (1) this will not increase the workload because traffics will not increase. (2) Even if scale (number of files) of homepage system increased, it will not influence to the check time and recovery speed.

The system of the present invention does not influence to browser. One can use current browser, and it is no need to download new client software. The system of the present invention has dynamic recovery function. If it finds alteration, it will replace automatically right away with the original web file. And one can set up automatic alert system. If it finds alteration, it will automatically send alert to the handy telephone or pager of system administrator. The system of the present invention is easy to install and not influence to current home page editor system. With the system of the present invention, it is allright (the user needs basic knowledge of web server management) installation of a public-web-server computer, installation of policy management system to current web side and simple setting.

With the system of the present invention, homepage editors can use their

accustomed tools, so without change of current environments they can design, build and update home pages. And they can automatically encipher newest web files of home page, add MAC and send them to web server.

With the system of the present invention, one can realize followings. (1) If there were alteration, altered web files will not sent to outside (accessed person). (2) If Hackers invaded to web server, they cannot do meaningful alteration enciphered web files.

There is another merit in the present invention of altar prevention system such that one can install this without complete change of current system. The financial impact will not so much as that it does not need special machine or technology. User can use current browser without any burden. (Because the data sent out to Internet are same as current page data.). That means completely no impact for Internet users.

Especially with using Chaotic Encryption System and Chaos MAM authentication technology, the following excellent results can be achieved.

High safety (It is new encryption system and is very little possibility to be deciphered).

High speed processing.

A little workload for system.

Possibility of real time processing (high speed of encryption, decryption and authentication check).

Zero impact for browser software.

Authentication check for anti-alteration is done at the time issued the send request of web file (ex. http) to client, and decipher process also done at that time, so those processing's require high speed. In this point, Chaotic Encryption System is the most suitable encryption system for them.